alert Technology and Manufacturing Companies Practice

Saul Ewing LLP

APRIL 2014

Heartbleed Bug Creates Risk for Businesses and Consumers

Authors:
Evan J. Foster
David S. Leone

SUMMARY

On April 8, 2014, several news agencies, including the New York Times and CNN, reported the discovery of a vulnerability in a core security protocol used by an estimated two-thirds of the world's servers. The vulnerability lies within the OpenSSL encryption technology used for conducting a multitude of internet communications including online transactions previously thought to be secure. Would-be hackers can exploit this flaw to obtain financial information, usernames, passwords, security keys and almost any other data without leaving a trace. Companies and individuals are urged to take steps to both secure their online accounts and assess their exposure to malicious activity. Companies and organizations that use cloud technology or other online services should understand what protections their service providers have put in place and investigate whether additional action is warranted.

The vulnerability, known by the moniker Heartbleed or the Heartbleed bug, was disclosed last week by a Google employee and an independent Finnish company named Codenomicon. According to the researchers, the vulnerability affects the Secure-Socket Layer (SSL) and Transport Layer Security (TLS) protocols, which are part of the OpenSSL 1.0.1 cryptographic technology. OpenSSL is widely used to secure thousands of websites, as well as provide security for mobile devices, virtual private networks and hardware.

While online service providers and tech companies scramble to deliver and apply patches, many systems are still at risk and have been for an estimated two years previously – since March 2012. Google, Amazon, Instagram and many other notable online businesses and app developers have already reportedly taken steps to secure their sites. Since the use of OpenSSL is so widespread, many smaller online companies, who may not have the resources of online giants, are still at risk. Patches need to be applied, compromised certificates need to be replaced, and passwords should be reset. This undertaking and auditing process will be difficult and burdensome. The patching process is likely to be further complicated where hardware is not connected to a network, such as industrial control equipment, which may require a physical connection to the affected equipment to apply the patch.

Saul Ewing has a team of attorneys, a network of independent cybersecurity professionals (including security and forensic data technology firms) and PR specialists to compile collaborative approaches and solutions to help protect the resources and property of the firm's clients. On the preparedness side, they are experienced at putting together response plans, reviewing insurance policies to assess whether cyber risks are appropriately covered and working with security specialists to review and identify technology weaknesses on behalf of clients.

Once the immediate threat has passed, this event may also provide an opportunity to review security incident response plans as well as vendor relationships for the appropriate contractual protections. If your business or organization does not yet have a plan in place, our attorneys will outline procedures and help develop a plan to prepare you for an external attack and reduce the risk of future intrusions.

In the event of a breach, our team of attorneys and network of external professionals work together to minimize exposure and protect client confidences. We provide counsel regarding liabilities potentially associated with the attack or breach and represent clients in related litigation when needed. We have experience in counseling clients on notification or reporting to customers/clients/patients as required by law or otherwise, and have worked collaboratively with crisis communications and public relations professionals to craft the appropriate responses. For more information on how the firm's cybersecurity team can help you assess your data breach risk, please contact Evan J. Foster, Christopher R. Hall, Joel C. Hopkins, Eric G. Orlinsky or Adam F. Kelson.

This Alert was written by Evan J. Foster, a member of the firm's Technology and Manufacturing Companies Practice, and David S. Leone, Director of Litigation Support Services. For more information, please contact Evan at 610.251.5762 or efoster@saul.com.